REMARKS

In the Final Office Action mailed on January 31, 2006, the Examiner rejected claims 1-16 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,321,752 to Iwamura et al. ("*Iwamura*") and "Pipelined 50 MHz CMOS ASIC for 32 Bit Binary to Residue Conversion and Residue to Binary Conversion" by Sathi Perumal et al. ("*Perumal*").

Claims 1-16 remain pending. Applicants have amended claim 2 to insert a period (".") to conclude the claim, and claims 1 and 14-16 to correct a typographical error. Support for the amendments to claims 1 and 14-16 can be found at least on page 28, line 27 of Applicants original disclosure, which states, "dq = d mod (q - 1)." Page 9, line 27 of the specification has been amended in a similar manner.

Applicants respectfully traverse the rejection of claims 1-16 under 35 U.S.C. § 103(a) as being unpatentable over *Iwamura* in view of *Perumal*. To sustain a rejection under 35 U.S.C. § 103(a) the Examiner must establish a *prima facie* case of obviousness by showing (1) that the applied prior art references, taken alone or in combination, teach or suggest all of the claim elements; (2) that there is motivation to modify the cited references to result in the claimed invention; and (3) that there is an expectation of success from modifying the cited references.

With respect to claim 1, *Iwamura* and *Perumal*, taken alone or in combination, do not establish a *prima facie* case of obviousness because they do not teach or suggest all of the claim elements. In particular, *Iwamura* at least fails to teach or suggest, "a first processing unit configured to obtain a residue number system representation of a value Cp^{dp} x B mod p or a value with p added thereto based on a residue number system

representation of a remainder value Cp = C mod p by p of said data C and a remainder value dp = d mod (p - 1) by (p - 1) of said parameter d," as recited in claim 1. The Examiner alleges that column 4, lines 25-27 of *Iwamura* teaches this limitation of claim 1. The relied-upon portion merely discloses a "computing unit to output $M_R = M \cdot R_R \cdot R^{-1} \bmod N$; representing the binary expression of e by $e = [e^t, e^{t-1}, \ldots, e^1]$" (Final Office Action at 14). The binary expression "e by $e = [e^t, e^{t-1}, \ldots, e^1]$," however, does not constitute "a residue number system representation of a value Cp^{dp} x B mod p or a value with p added thereto based on a residue number system representation of a remainder value Cp = C mod p by p of said data C and a remainder value dp = d mod (p - 1) by (p - 1) of said parameter d," as recited in claim 1. More specifically, a residue number representation uses, for example, remainder values $[x_1, x_2, \ldots, x_n]$ to represent a number x as calculated by $x_1 = x \bmod a_1$, $x_2 = x \bmod a_2$, . . ., $x_n = x \bmod a_n$, where a_1, a_2, . . ., a_n are moduli. Accordingly, *Iwamura*'s binary expression for e does not disclose Applicants' claimed "residue number system representation of a value Cp^{dp} x B mod p or a value with p added thereto based on a residue number system representation of a remainder value Cp = C mod p by p of said data C and a remainder value dp = d mod (p - 1) by (p - 1) of said parameter d." Therefore, *Iwamura* does not disclose "a first processing unit configured to obtain a residue number system representation of a value Cp^{dp} x B mod p or a value with p added thereto based on a residue number system representation of a remainder value Cp = C mod p by p of said data C and a remainder value dp = d mod (p - 1) by (p - 1) of said parameter d," as recited in claim 1.

In addition, for reasons similar to those discussed above for the "first processing unit," *Iwamura* also fails to teach or suggest "a second processing unit configured to

obtain a residue number system representation of a value Cq^{dq} x B mod q or a value with q added thereto based on a residue number system representation of a remainder value Cq = C mod q by q of said data C and a remainder value dq = d mod (q - 1) by (q - 1) of said parameter d," as recited in claim 1. Likewise, *Iwamura* also fails to teach or suggest the claimed "a third processing unit configured to obtain a residue number system representation of an integer m' congruent with C^d mod (p x q) based on both the residue number system representations obtained by said first and second processing units." More specifically, *Iwamura* make no mention of using residue number system representations from the first and second processing units to "obtain a residue number system representation of an integer m' congruent with C^d mod (p x q)," as recited in claim 1.

Perumal fails to cure the above-noted deficiencies of *Iwamura*. The Examiner alleges that *Perumal* discloses "the Residue to Binary conversion [page 456, lines 23-25 'if two residue number Z1 and Z2 are known, then the binary number equivalent B can be calculated from (13)']" (Final Office Action at 4). *Perumal* merely discloses a CMOS ASIC for binary-to-residue conversion and residue-to-binary conversion (*Perumal*, pp. 454-55). Such teachings, however, do not constitute "a first processing unit configured to obtain a residue number system representation of a value Cp^{dp} x B mod p or a value with p added thereto based on a residue number system representation of a remainder value Cp = C mod p by p of said data C and a remainder value dp = d mod (p - 1) by (p - 1) of said parameter d," as recited in claim 1. Furthermore, for reasons similar to those presented above for the "first processing means," *Perumal* fails to teach either "a second processing unit configured to obtain a residue number system

representation of a value Cq^{dq} x B mod q or a value with q added thereto based on a residue number system representation of a remainder value Cq = C mod q by q of said data C and a remainder value dq = d mod (q - 1) by (q - 1) of said parameter d" or "a third processing unit configured to obtain a residue number system representation of an integer m' congruent with C^d mod (p x q) based on both the residue number system representations obtained by said first and second processing units," as recited in claim 1. Thus, *Iwamura* and *Perumal*, alone or in combination, fail to teach or suggest each and every element of claim 1. Accordingly, the rejection of claim 1 under 35 U.S.C. § 103 should be withdrawn.

While of different scope than claim 1, independent claims 14-16 recite subject matter similar to that of claim 1 already discussed. Applicants therefore assert that claims 14-16 are allowable at least for the reasons presented above for claim 1. In addition, Applicants assert that claims 2-13 are allowable at least based on their dependence from allowable claim 1.

Applicants respectfully request that this Amendment under 37 C.F.R. § 1.116 be entered by the Examiner, placing claims 1-16 in condition for allowance. Applicants submit that the proposed amendments of claims 1, 2, and 14-16 do not raise new issues or necessitate the undertaking of any additional search of the art by the Examiner, since all of the elements and their relationships claimed were either earlier claimed or inherent in the claims as examined. Therefore, this Amendment should allow for immediate action by the Examiner.

In view of the foregoing remarks, Applicants submit that this claimed invention, as amended, is neither anticipated nor rendered obvious in view of the prior art

references cited against this application. Applicants therefore request the entry of this Amendment, the Examiner's reconsideration and reexamination of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: May 1, 2006

By: 
Patrick L. Miller
Reg. No. 57,502